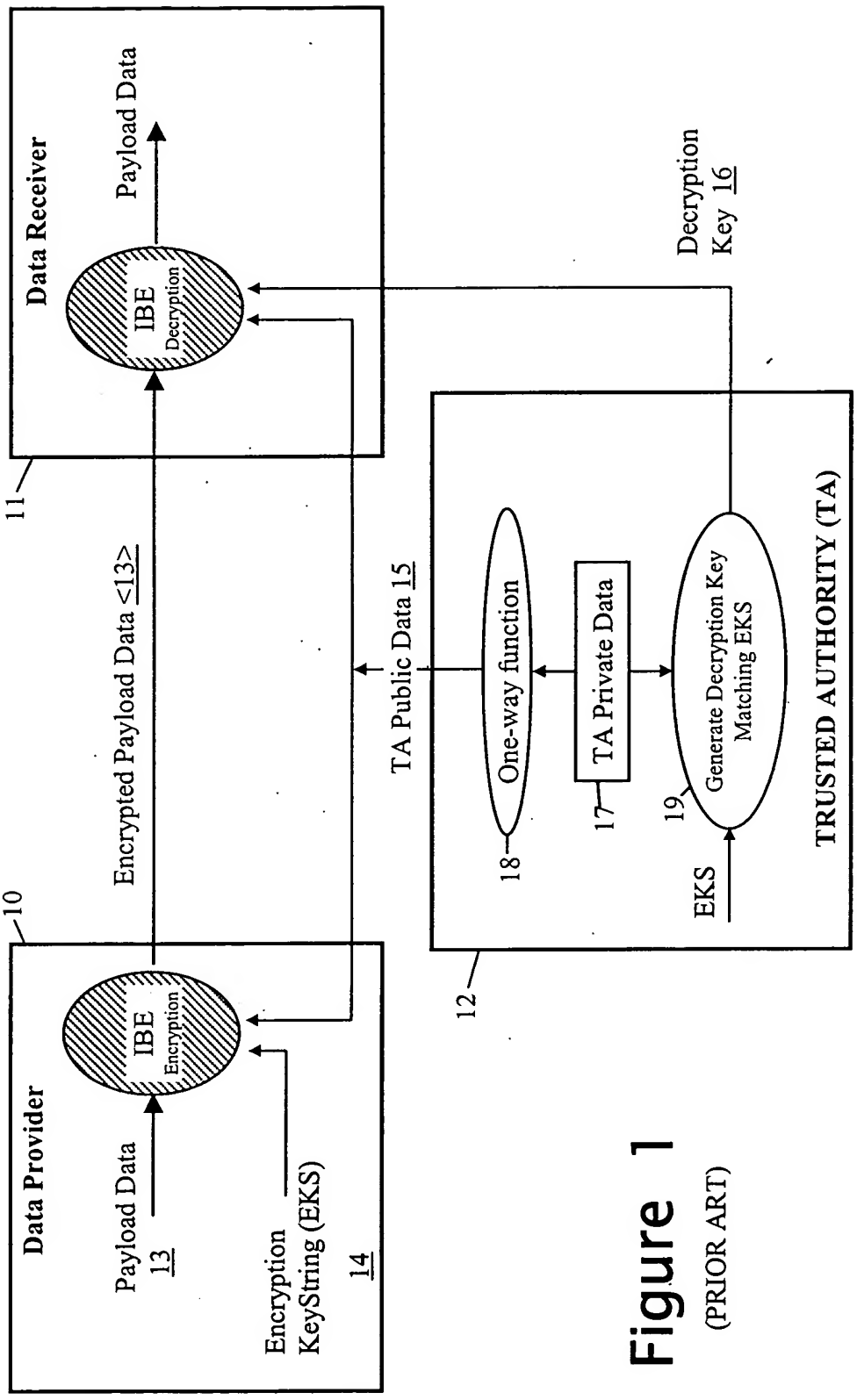
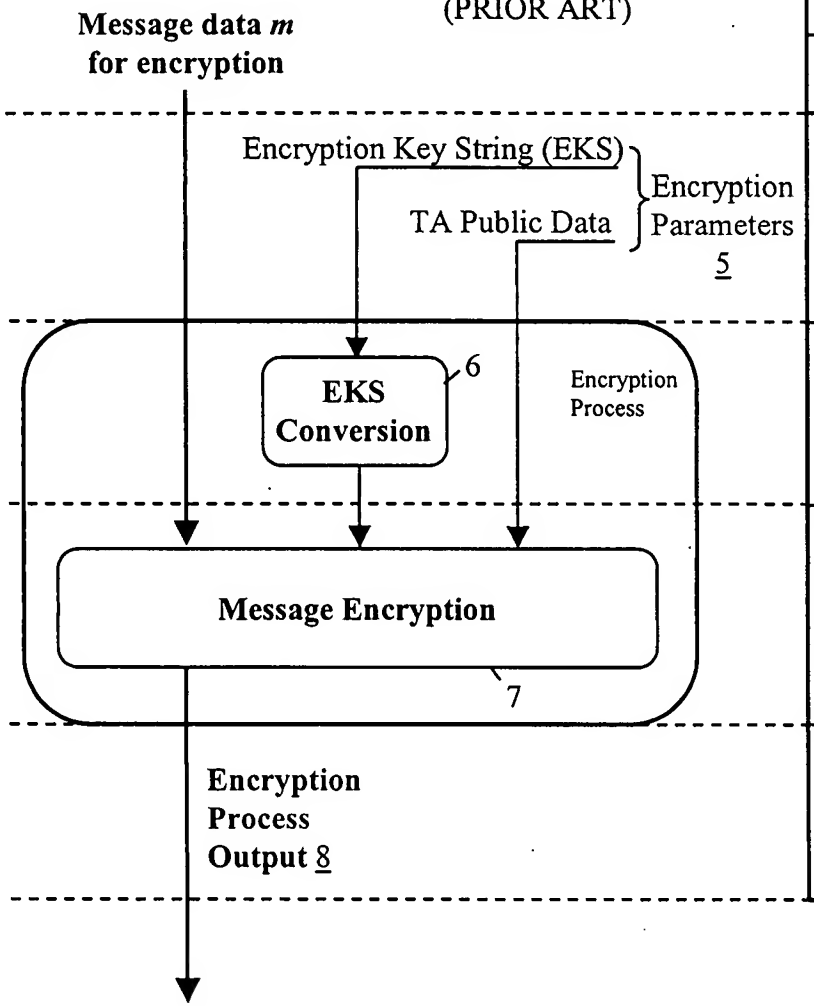


Figure 1
(PRIOR ART)

Figure 2

(PRIOR ART)



	Identifier-Based Method		
	Quadratic Residuosity	Bilinear Mappings $\hat{e}: G_1 \times G_1 \longrightarrow G_2$	RSA Based
Encryption Key String (EKS) / TA Public Data (Encryption Parameters 5)	EKS Modulus N	EKS (P, sP) where P is in G_1, s is secret of TA	EKS Modulus n
EKS Conversion 6 / Encryption Process	$K = \#(\text{EKS})$	"Map-to-point" hash $Q_{ID} = H_1(\text{EKS})$ where $H_1: \{0,1\}^* \longrightarrow G_1$	e = #(EKS)mod n
Message Encryption 7	For each bit: $s_+ \equiv (t_+ + K/t_+) \bmod N$ $s_- \equiv (t_- - K/t_-) \bmod N$	$V = m \oplus H_2(t\,(sP, rQ_{ID}))$ where: $H_2: G_2 \longrightarrow \{0,1\}^*$ r is a random number	$m^e \bmod n$
Encryption Process Output 8	For each bit: s_+ s_-	V, $U\,(= rP)$	$m^e \bmod n$
(knowledge of EKS and TA concerned also needs to be available)			

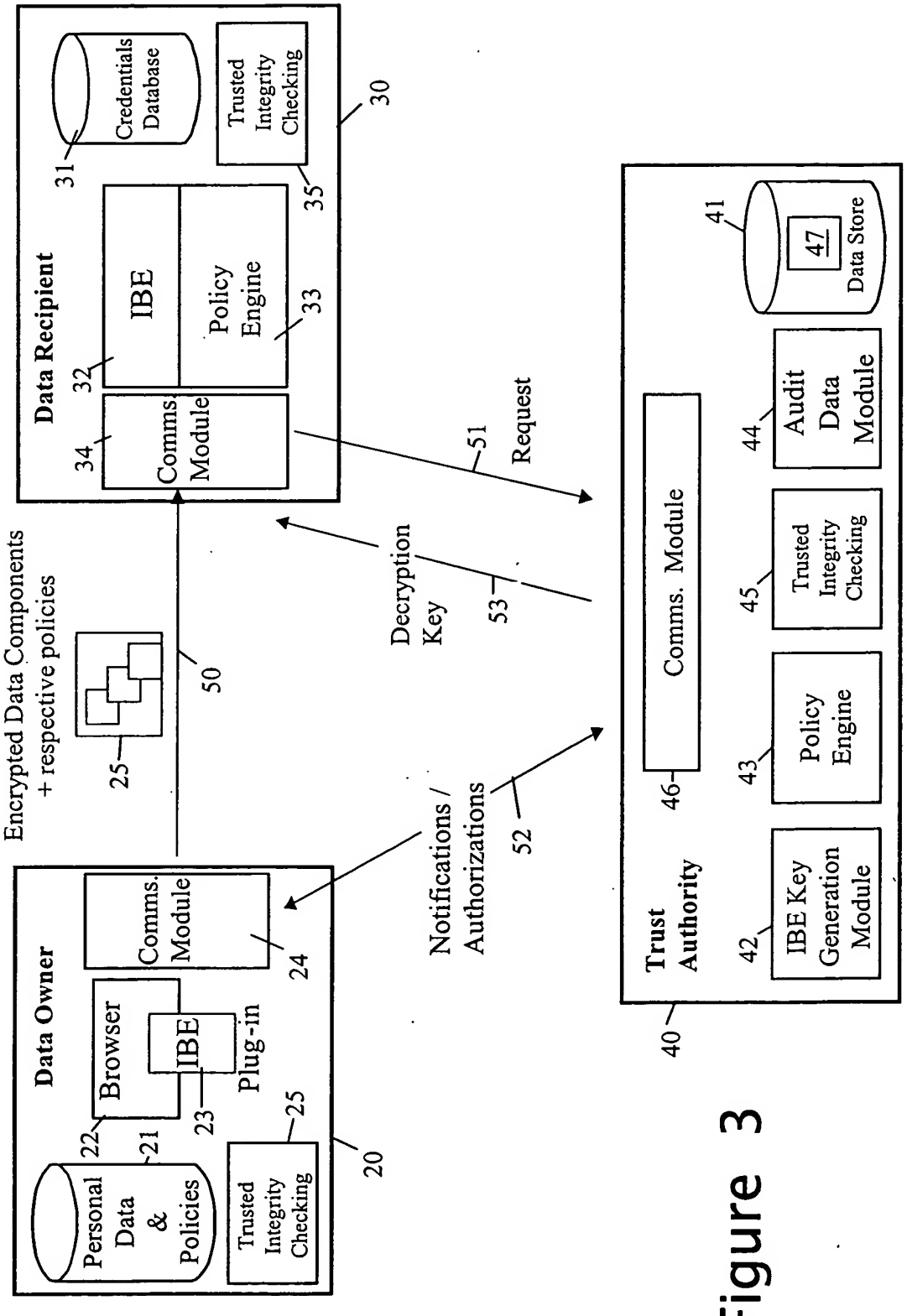

Data Owner
Personal Data & Policies
Browser
IBE
Plug-in
Trusted Integrity Checking
Comms. Module
20
21
22
23
24
25
Encrypted Data Components + respective policies
50
Data Recipient
Credentials Database
31
IBE
32
Policy Engine
33
Trusted Integrity Checking
35
Comms. Module
34
30
51
Request
Decryption Key
53
Notifications / Authorizations
52
Trust Authority
40
Comms. Module
46
IBE Key Generation Module
42
Policy Engine
43
Trusted Integrity Checking
45
Audit Data Module
44
41
47
Data Store

Figure 3

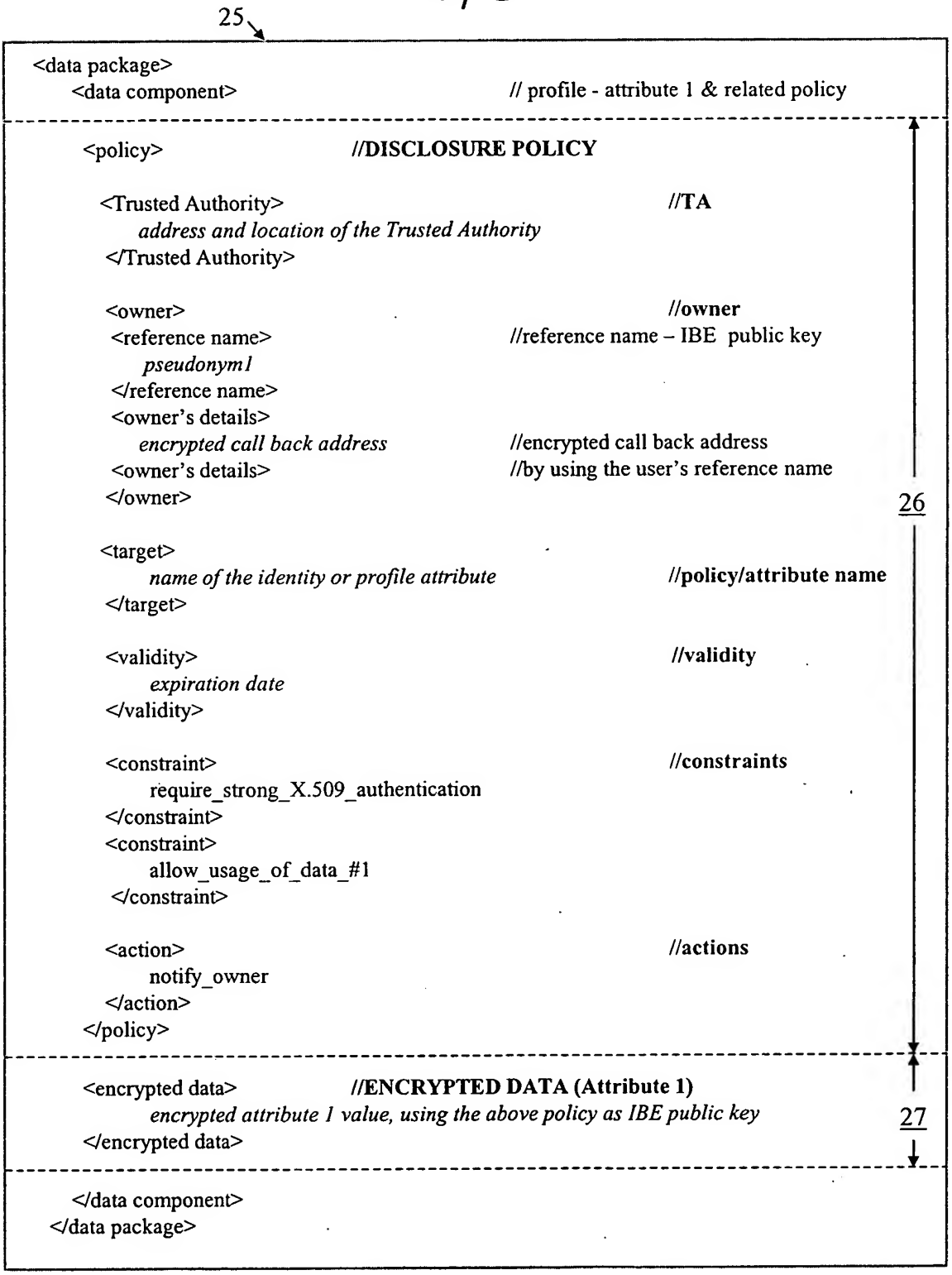

25
<data package>
<data component> // profile - attribute 1 & related policy
<policy> //DISCLOSURE POLICY
<Trusted Authority> //TA
address and location of the Trusted Authority
</Trusted Authority>
<owner> //owner
<reference name> //reference name – IBE public key
pseudonym1
</reference name>
<owner's details>
encrypted call back address //encrypted call back address
<owner's details> //by using the user's reference name
</owner>
26
<target>
name of the identity or profile attribute //policy/attribute name
</target>
<validity> //validity
expiration date
</validity>
<constraint> //constraints
require_strong_X.509_authentication
</constraint>
<constraint>
allow_usage_of_data_#1
</constraint>
<action> //actions
notify_owner
</action>
</policy>
<encrypted data> //ENCRYPTED DATA (Attribute 1)
encrypted attribute 1 value, using the above policy as IBE public key
</encrypted data>
27
</data component>
</data package>

Figure 4

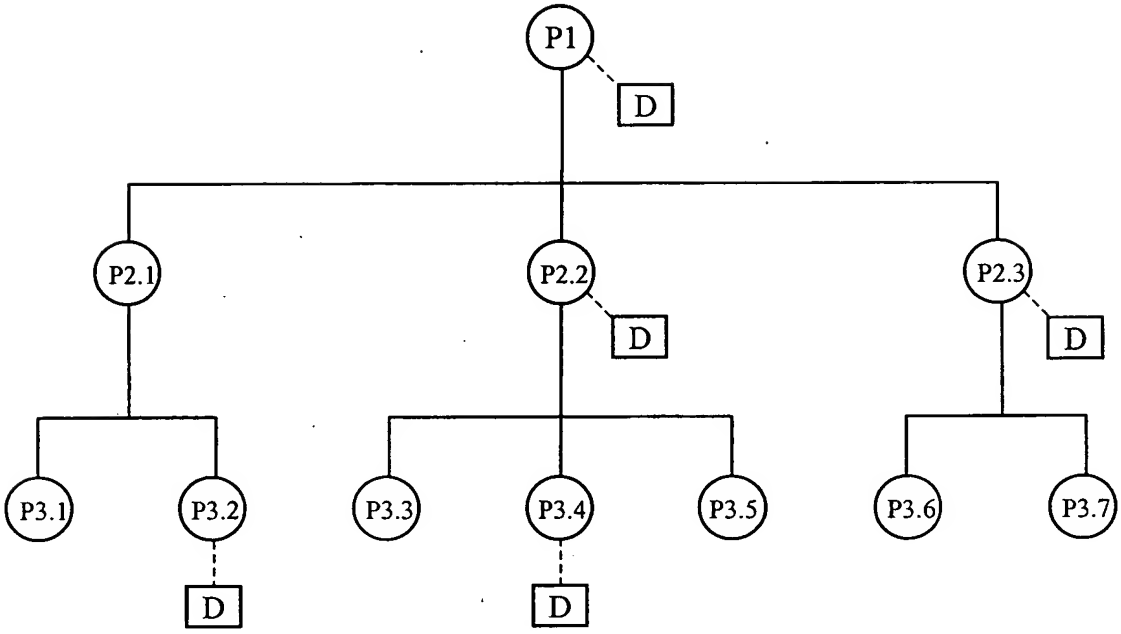


Figure 5